# Mobile App Programming II Bibliography Part I

Matt Zagame

April 10, 2022

## References

[1.1] Metcalf, David, Milliard, Sharlin T.J., Gomez, Melinda, and Schwartz, Michael. Wearables and the internet of things for health: Wearable, interconnected devices promise more efficient and comprehensive health care. *IEEE Pulse*, 7(5):35–39, 2016.

> **Abstract:** The Internet of Things (IoT) and its implementation into wearable smart devices has proven to provide a host of benefits to human lifestyle and health. IoT devices are ushering in a wave of innovation by allowing us to connect nearly any device that we might use on a daily basis to a pervasive smart network that can be controlled from our fingertips. Also, new wearable and embeddable tech makes staying connected even easier and provides great health care benefits. For example, the average user is able to monitor their own health, and health care providers have access to more tools (such as AR) to offer better care. So as long as IoT and wearables remain useful to most users, this emerging technology could certainly be here for the long-term.

[1.2] Nield, David. What is web3 and why should you care? *Gizmodo*, 2021.

> **Abstract:** Web3 is being coined as the evolution of the Internet. However, its aim is to take a step back from the over-centralization of the current web (Web 2.0) to the early days of the Internet which was more

decentralized. Essentially, striking a balance between Web 1.0 and the current web that is primarily controlled by large corporations. This is done by layering blockchain technology onto the web to allow data transfers to be done on an encrypted network that is not owned nor operated by any central authority. Currently it is too early to tell whether this will be possible to implement in a truly decentralized way and on such a large scale. However, if implemented, it could change the way information moves across the Internet forever.

[2.1] Davies, Aran. How to build an investment portfolio app. *DevTeam.Space*, 2019.

**Abstract:** The market for personal finance applications has been on the rise over the past few years and is expected to continue rising at a compounded annual growth rate of 6.4% from 2017 to 2023. The ease of managing your portfolio and monitoring your spending right from your mobile device has enticed a new generation of investors and people who are less involved with finances to gain more control over their financial goals. In order to create a useful personal finance app, there are a several important steps that must be taken. Some of these include: planning features and a minimum viable product, creating a development roadmap, implementing industry-standard or better APIs for a smooth and secure app experience, team building and organization, etc.

[2.2] Kirkpatrick, Keith. Monetizing your personal data. *Communications of the ACM*, 65(1), 2022.

**Abstract:** In the modern digital age of the Internet, it has become common for most online services that we use in our everyday lives to keep a record of the data that we provide. Large companies such as Google, Facebook, Amazon, etc., all use this data to target advertisements towards us in hopes to get our attention and ultimately turn a profit. In essence, our

data is being traded behind the scenes so that these companies can sell us their products. But what if consumers were the ones in control of the data that was up for sale? While individuals' data is not necessarily all that expensive, giving end users the ability to control which data gets shared could lead to a more fair and trusted internet advertising market. In the future, data brokers could offer up this kind of information exchange which could largely alter our interactions online.

[3.1] Kim, Dongyeon, Park, Kyuhong, Park, Yongjin, and Ahn, Jae-Hyeon. Willingness to provide personal information: Perspective of privacy calculus in iot services. *Computers in Human Behavior*, 92:273–281, 2019.

**Abstract:** The increased development and production of IoT devices has provided many personalized benefits to the average consumer. However, a more personalized experience comes at the expense of more personal information. This study seeks to determine how willing consumers are to provide personal information at the risk of a breach of their own privacy using the privacy calculus theory. Data was collected via a survey of over 150 people with exposure to IoT devices in a few different areas such as healthcare, smart home, and smart transportation. In summary, perceived benefit was met with more people willing to provide personal information, whereas perceived risk did not significantly impact the data. The exception being IoT in healthcare where privacy risk is high, in which case people were less willing to provide personal information despite the less personalized experience.

[3.2] Polkadot.ERI. One article to understand the past, present, and future of web 3.0. *Medium*, 2021.

**Abstract:** In the early days of the World Wide Web, information and entertainment services such as AOL, Google, and Yahoo were among the most popular and

profitable services as the web's user base largely consisted of content consumers. After over a decade of what was known as Web 1.0, Web 2.0 brought in an era of content creators that share and post content on various platforms such as YouTube, Facebook, Twitter, etc, which continues to exist to this day. Originally, Web 3.0 was to be known as the Semantic Web, where devices would process and share data contextually and conceptually via machine learning, ideally in an IoT style network. Given the rise of blockchain technology, the focus of Web 3.0 has shifted to democratizing and restoring privacy on the Internet. While Web 3.0 is still being defined, it has the potential to mitigate the issues with the current web and bring about the perfect internet, where users can be both content consumers and creators without any fear of losing the rights to their digital identity.

[4.1] Jacksi, Karwan and Abass, Shakir M. Development history of the world wide web. *Int. J. Sci. Technol. Res*, 8(9):75–79, 2019.

**Abstract:** This article discusses the different versions of the web from Web 1.0 to Web 3.0 which at the time was known as the semantic web. Web 1.0 began in the early 90s and was a static, read-only type of web where users could simply search for and read information off of HTML based web pages. The only people who created content for the web were developers with knowledge of HTML, CSS, etc. Web 2.0 emerged around 2004 and became known as the read-write web. By this point in time users could interact with more dynamic web pages, and through the use of various platforms publish a variety of their own content. However, this web also brought with it the issue of data centralization. Originally, Web 3.0 was projected by Tim Berners-Lee to be the era of a machine-learning based contextual web. This evolution of the web can be thought of as an infrastructure that is made up of many layers. Some of these layers include, the semantic web stack, ontology and rela-

tion of data, resource description frameworks, and OWL, most of which are developed by the W3C.

[4.2] Mühle, Alexander, Grüner, Andreas, Gayvoronskaya, Tatiana, and Meinel, Christoph. A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30:80–86, 2018.

**Abstract:** The emergence of blockchain technology has opened the door for decentralized solutions to data transfer and information exchange. Currently, users need to sign up for services in order to be identifiable on the web. Corporations being in control of user data is the reason why many are looking into self-sovereign identity solutions for the web. Originally coined by the W3C, a self-sovereign identity is an identity management system where individuals have full control over their digital identity. Blockchain's decentralized consensus mechanisms have the potential to be the solution to online identity management. The three main requirements for a self-sovereign identity are security, controllability, and portability. In terms of the current SSI architecture, four components are analyzed in relation to blockchain tech; these are, identification, authentication, verifiable claims, and attribute storage.

[5.1] Bloomfield, Brian P. and Coombs, Rod. Information technology, control and power: The centralization and decentralization debate revisited*. *Journal of Management Studies*, 29(4):459–459, 1992.

**Abstract:** The article discusses the debate between centralization and decentralization of computers within organizations and analyzes the implications this has on power. In the sense of this debate, power is directly related to the control of information. A sovereign view of power establishes the notion that you either have power or something else has power over you, ergo it can be seen as a zero-sum game. Likewise, centralization and decentralization must both

exist in a system of equilibrium. However, the centralization of information is more often found towards the top of organizational hierarchies. It is also argued that computers are not responsible for the centralization or decentralization of power, but tend to reinforce the power of dominant actors. Furthermore, organizational information systems are better managed by computers and those who can use computers to their advantage. The article also focuses on how information systems are being developed for use in the National Health Service.

[5.2] Nofer, M., Gomber, P., and Hinz, O. et al. Blockchain. *Bus Inf Syst Eng*, 59:183–187, 2017.

**Abstract:** One of the biggest problems with financial markets is tracing back ownership in long transaction chains. Intermediaries are responsible for carefully and accurately recording transactions so that everything is in proper order. Blockchain technology aims to overcome the risks involved in these legacy financial situations by replacing trust in people with trust in a complex mathematical structure. Blockchains are an append-only, immutable type of data structure that operates and is maintained by various nodes. Nodes validate information on-chain via a consensus mechanism in which each node must agree on the validity of the block before it is added to the chain. Since blockchains do not rely on third parties to verify information, they are inherently more secure and allow for a trustless transaction of information. Today, blockchain is most commonly implemented in cryptocurrencies. Blockchain, naturally, could play a large role in the financial sector due to its ledger-like properties being able to work in real-time. In the future, innovative entrepreneurs who are willing to work with cryptocurrencies may allow blockchain to flourish.

[6.1] Greengard, Samuel. What is the cost of living online? *Commun. ACM*, 64(12):23–25, nov 2021.

**Abstract:** As the digital age continues to expand and take over more of our daily lives, the cost of living online has also seen a sharp uptick. Many popular social networking platforms such as YouTube, Facebook, Zoom, TikTok, etc., have experienced great increases in user interaction most recently during the pandemic. The increased demand for more bandwidth has brought with it concerns about energy consumption associated with our projected internet usage. Along with existing internet technologies such as video streaming, which reportedly accounts for 45all internet activity today, emerging technologies such as AI, machine learning, blockchain, and IoT are likely to raise energy usage considerably more. It is imperative that we are able to accurately measure energy consumption, and to devise solutions that enable devices to be more energy-efficient. While bandwidth fears are becoming more apparent, and justifiably so, it has been deemed incredibly unlikely that bandwidth-heavy activity such as video streaming could ever take down the Internet.

[7.1] Gasser, Urs and Almeida, Virgílio. Futures of digital governance. *Commun. ACM*, 65(3):30–32, feb 2022.

**Abstract:** Advances in digital technology continues to rapidly redefine society. Many sectors of society have undergone digital transformations which have brought with them both new opportunities and challenges. In many parts of the world, modern institutions and processes lack the ability to keep up with the ethical, legal, and societal issues that emerge from digital technologies. This is the basis for digital governance. In short, digital governance is a framework that helps to manage the risks associate with digital technologies. Digital governance also has many meanings. It is unclear whether new digital technologies will create a need for new governance models or if they will be dependent on existing models. In the case of the Internet, novel governance models such as

an organization in charge of the reservation of IP addresses (ICANN) was established. Given the scale and scope of emerging digital technologies, it is probable that path dependencies will need to be avoided. As such, an investment in the interoperability of social sciences and humanities should help bring communities together and foster useful innovations in digital governance.

[7.2] Monroe, Don. Accelerating ai. *Commun. ACM*, 65(3):15–16, feb 2022.

**Abstract:** AI and machine learning applications have ushered in a new paradigm for computing. The ability for neural networks to process billions of parameters from massive datasets is a huge computational advancement, yet it also comes with huge costs. Running a neural network at such a scale can cost millions of dollars with high energy consumption and carbon emissions. Sourcing energy from solar instead of coal is a more eco-friendly alternative, however this comes with trade-offs that must first be quantified. Thus, a primary focus in the machine learning industry is on efficiency. In most cases, GPUs (Graphics Processing Units) have demonstrated that they are more efficient at handling neural network computations than CPUs, given their parallel processing structure and high memory bandwidth. Alongside GPUs, many implementations of Google's TPUs and ASICs (Application Specific Integrated Circuits) can also be found. Furthermore, opportunities for hardware innovations are also on the rise. Some hardware companies are proposing lowering precision at the instruction set level in order to skip over unnecessarily small values and boost efficiency. Looking ahead, it is paramount that the acceleration of neural networks is environmentally sustainable.

[8.1] Cerf, Vinton G. Preserving the internet. *Commun. ACM*, 65(4):5, mar 2022.

**Abstract:** The value of the Internet has become far greater as the complexity of its ecosystem has expanded. The number of devices and users connected to the Internet has increased rapidly over the past few decades and continues to rise. As the Internet improves and adapts to new technologies, governments, corporations and other entities that rely heavily on the Internet have had great interest in its preservation. The Internet, being publicly open and accessible to anyone, currently serves both beneficial and harmful purposes. Therefore, it is imperative to work towards preserving only beneficial uses and preventing any harmful abuse. Several aspects of the technical infrastructure can be improved to provide better security, such as DNSSEC, two-factor authentication, transport layer security, end-to-end cryptography, stronger identity control, etc. Currently the Internet is fragmented by legal jurisdictions which are subject to control by various governments. If the Internet is to be safe and secure while preserving its openness, cooperation between jurisdictions will be most likely in the decades to come.

[8.2] Roach, John. Microsoft finds underwater datacenters are reliable, practical, and use energy sustainably. *Microsoft Innovation Stories*, 2020.

**Abstract:** Project Natick is the name of Microsoft's deep-sea datacenter project which also fittingly powers the Microsoft Azure cloud service. The datacenter was recently retrieved after having been submerged for two years in the Northern Isles. During this time, Microsoft's team was able to monitor the performance of the data center and found that only 8 of the 855 servers had gone offline. The idea behind the project was to efficiently provide cloud based services to many users within 120 miles of the coast where the datacenter was located. As it turns out, running the servers underwater improves energy efficiency by mitigating heat exchange and keeping the servers cool.

Retrieving the data center took a full day and revealed a thin coating of algae and barnacles that had formed on the outside of the datacenter which was then powerwashed and cleaned off. The project's team was impressed to find that the underwater datacenter had a one-eighth failure rate compared to the datacenters on land. In addition, freshwater resources were not disturbed at any point during operation. Going forwards, the team at Microsoft has expressed optimism in continuing to operate their services in the most secure and energy efficient ways possible.

[9.1] Tobin, Andrew, Reed, Drummond, and Windley, Phillip J. The inevitable rise of self-sovereign identity. *The Sovrin Foundation*, 2017.

**Abstract:** Online identities have come a long way, however they still do not function in a way that is as automatic as the Internet routes information between devices. In the current web model, online identities are tied to various services and platforms such as social media. A self-sovereign identity on the Internet would allow a user to have an identity relationship without the need for authorization from another entity (e.g. Google, Facebook, Twitter). The Internet was not built with identity in mind. Sovrin is therefore proposing to redefine online identity functions with self-sovereign identity by leveraging blockchain technology. A self-sovereign identity must satisfy three basic requirements, security, control and portability. Identity information must be kept secure and private unless expressly shared by the owner, and must be accessible to the user at any time. In a way, SSI is a digital record who's owner can add to or ask others to add to at any time. Connecting to the Internet's identity layer will enable instant access to any and all shared data on the network. Sovrin explains how distributed ledger technology makes this possible with distributed key management and encrypted peer-to-peer sharing of claims.

[9.2] Greengard, Samuel. Can ai learn to forget? *Commun. ACM*, 65(4):9–11, mar 2022.

**Abstract:** Retraining machine learning models is an expensive and time-consuming process. Instead of having to build completely new models, a new method of "machine unlearning" using specialize techniques could allow for rebuilding models on the fly. Selectively choosing which data to delete is not an easy task, therefore algorithms are often left in tact and models are rebuilt from scratch. Several privacy techniques have been proven to prevent sensitive data from ending up in a database but cannot remove it. Another key space that researchers have been focusing on is the randomness, or stochasticity involved in minor changes to input data which sometimes lead to greatly different results. One proposed method to solve the machine unlearning problem is known as the SISA (Sharding, Isolated, Sliced, Aggregated) method. This method divides the training data into multiple disjoint shards and does training on each of the isolated shards, after which they are combined back together onto the main training set with elements successfully removed. The sharding method has proven to work efficiently and exactly as if the model had never learned the data in the first place. In the future, machine unlearning tasks should allow the removal of data while confidently maintaining a valid model.